Messaging fatigue – why you shouldn't ignore cyber alerts

Sophie Duffy
Claims Solicitor

Maintaining a high level of cyber security is crucial to safeguarding sensitive information and protecting critical systems in your practice.

Unfortunately, the challenge of alert fatigue can undermine the effectiveness of security operations. Cyber fraud risk messaging has become a constant, and it is tempting to ignore reminders and security alerts and assume that if your practice's cyber security systems are up to date then you are safe. Cyber criminals exploit this fatigue with phishing emails and social engineering scams becoming more sophisticated.

Solicitors are obvious targets

Conveyancing transactions are obvious targets for cyber criminals. There are vulnerable times in the property transaction process when the risk is heightened, including when the deposit is due. The risk of cyber fraud further increases in the weeks before settlement, when solicitors may not be corresponding regularly with their clients.

Solicitors are often surprised that their client acted on a fraudulent email in circumstances where they have clearly communicated that the settlement funds would only be requested just before settlement.

The first email your client receives from a cyber criminal will likely not be asking them to transfer funds. Instead, the criminal may send a series of emails over days or weeks, slowly building rapport with the client. The emails can be entirely convincing, reflecting the communication style of the solicitor, showing a genuine interest in the client, and addressing any concerns they may have about the upcoming purchase or process.

Whilst clients may have been warned by the solicitor about the potential of cyber attacks and fraud, during this phase of a cyber attack clients assume they are communicating with the solicitor and nothing may appear suspicious.

In a recent claim, an email sent by a cyber criminal purported to provide the practice's trust account details including a warning at the footer of the email advising the client to always call before arranging payment to the practice's trust account, and provided a mobile number to call. The same fraudulent mobile number was added to the email signature of the solicitor and was identified as the phone number to use in urgent circumstances.

Despite clients being warned by the practice about cyber attacks and fraudulent transactions, most are inexperienced when it comes to purchasing a property. An early request for settlement funds, or changing the bank details from PEXA to another number or account, do not immediately raise any red flags with them.

There is little authority in Australia regarding a solicitor's liability in the context of a cyber breach and subsequent payment redirection fraud, or the extent of a solicitor's duty to take precautions to prevent the risk of cyber fraud. The more steps the solicitor takes to address the risk, and the better the systems the practice has in place, the more defensible the claim.

How to keep you and your clients secure

- Have a conversation with your client about cyber fraud risk at the beginning of the engagement
- Record these conversations in a file note
- Include references to cyber fraud risk and how it can be avoided in initial correspondence
- Remind clients of cyber security issues and warnings regularly throughout the course of the transaction
- Don't assume that the client will take steps to protect their own interests

Cyber risk doesn't have to be complex or difficult. Weave cyber security messages into client correspondence and set up practices internally to remind staff. For many practices a cyber claim may be their first claim with Lawcover, and it can be difficult to grapple with an allegation of negligence when both the solicitor and the client are the victims of a cyber attack.